

CITY OF SAN ANTONIO



Administrative Directive

AD 7.8D Account Access Management

Procedural Guidelines

Guidelines to control access to City data and IT resources.

Department/Division

Information Technology Services Department (ITSD)

Effective Date

July 6, 2009

Project Manager

John Byers, Chief Information Security Officer (CISO)

Purpose

Access to City of San Antonio (COSA) information technology (IT) resources must be controlled in a manner that helps protect the confidentiality, integrity, and availability of valuable information resources. Account access management is essential to the management of information because it assures the integrity, origin of data, and guarantees that information is genuine (this process is known as non-repudiation). COSA shall control account access to information resources as prescribed by the data or system owner.

Policy

This directive provides information on controlling access to City data and IT resources and is the companion directive to the User Account Management Directive. For the data/systems where the ownership rest solely with the Information Technology Services Department (ITSD), control of account access will be commensurate with the sensitivity of the information.

Policy Applies To

☐ External & Internal Applicants

☒ Current Temporary Employees

☒ Current Full-Time Employees

☐ Current Volunteers

☒ Current Part-Time Employees

☒ Current Grant-Funded Employees

☒ Current Paid and Unpaid Interns

☒ Police and Fire Academy Trainees

☒ Uniformed Employees Under Collective Bargaining Agreements

Definitions

Account Access Management (AAM)

Governs the administration of entry into City IT networks. Account access management differs from “user account management” (UAM) in that AAM does not address the issues associated with a user account, but instead addresses all matters associated with the management of access to resources and systems.

Policy Guidelines

General Guidelines

- A. While information is normally accessed through a user account, the control of the access is the responsibility of account access management. Account access management relies on system and business owners to determine which access controls should be placed on the systems and information for which they are responsible. ITSD personnel assigned administrative duties for systems are responsible for aligning the business/system owner access requirements with corresponding access controls to provide access control management.

Requirements

- B. Four general drivers pressure COSA to ensure that their users are eligible to access services: (1) funding sources, (2) ethical obligations, (3) legal requirements, and (4) prudent stewardship.
1. *Funding sources* (e.g., Federal and state government appropriated funds) direct that monies must be used to support COSA missions. In some circumstances, these sources dictate specific purposes for the monies provided.
 2. *Ethical obligations* involve the protection of privacy, intellectual property, and other “strategic” information. Unauthorized disclosure of these data may result in identity theft or other negative consequences. While some of these areas have established practices, others are emerging concerns.
 3. *Legal requirements* stem from statutory obligations, mostly related to personnel records, public health information, tax records, and other classified data. Among the regulations affecting access are the Health Insurance Portability and Accountability Act (HIPAA), and the Gramm-Leach-Bliley (GLB) Act. Service associations also enforce rules under which members must operate, such as those established by the Electronic Payments Association.
 4. *Prudent stewardship* involves access to data not protected by statute or without formal standards, such as information that can be combined to provide fodder for stalkers or that can cause embarrassment to individuals or to the City. These

data might contain personal information, such as social security numbers, or any other potentially damaging information. Open data access directives and open records laws affect decisions made about protecting data.

Control of Access

C. Basis for Granting Access

1. All access to any information within COSA shall be on based factors including but not limited to compliance, best practices as established by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), or Federal, State, and local statutory requirements.

D. Documentation of Access Control Requirements and Access Permission

1. Access control requirements and permissions for identified groups of users shall be clearly documented in organizational directives, procedures, and guidelines. Access controls are and should be both logical and physical yet with the blending of both types of controls being preferable.
2. The CISO and IT security staff will assist departments with their documentation to ensure accuracy and correctness.

E. Dissemination of Permissions

1. Because of potential misuse concerns, dissemination of the specific contents of the access controls and access permissions shall be strictly limited to personnel who have an authorized need-to-know determined by business owners and system administrators.
2. Members of large user groups with similar permissions may be informed of the general level of their access permissions.

F. Recipients Minimum Alignments to Protect Information

1. COSA access controls shall be aligned to provide the necessary assurance for the classifications that have been placed on information, whether the information has been generated by COSA or obtained from outside sources. Federal, State, and other government organizations maintain rigorous standards on accessing sensitive, operational, personal, and financial information. The City, in like manner, shall ensure that the same access controls are applied to like information.
2. Access controls are not limited to electronic media but shall extend to cover the physical access controls necessary to protect all information. Converting electronic media to another form, whether it is paper storage, tape storage, or

	<p>other media form does not declassify or remove the responsibility to provide access control. Electronic media, which has been converted, must be afforded the same level of protection that would be provided by the electronic access controls.</p> <p>3. <i>Example:</i> A document, which has been printed, must be protected through a process of manual access controls. Access controls may include storage of the information in an approved security container or protecting it from easy viewing by placing the information in a file folder. Depending upon the sensitivity of the information, destruction of the information may require burning or shredding.</p> <p><u>Training</u></p> <p>G. All COSA employees shall receive training regarding their responsibilities for complying with this directive. This directive shall be made available online to all COSA employees with cross references from ITSD websites.</p> <p><u>Exceptions</u></p> <p>H. Guidance for requesting exceptions to or deviations from this directive is outlined in <i>AD 7.5A Establishing IT-Related Directives</i>.</p>
Roles & Responsibilities	
<u>Chief Information Security Officer</u>	<p>A. Review this directive annually, at a minimum, for both consistency and accuracy</p> <p>B. Interpret and apply this directive under the direction of the Chief Information Officer (CIO) and/or the Chief Technology Officer (CTO), as appropriate</p> <p>C. Modify or amend this directive at any time pending formal review and approval as defined in <i>AD 7.5A Establishing IT-Related Directives</i></p> <p>D. Provide adequate notice of any such modifications or amendments</p> <p>E. Ensure the current version of this directive is posted in a public location accessible to all authorized City personnel</p> <p>F. Oversee and monitor all training</p>
<u>Departments</u>	<p>A. Responsible for any disciplinary action taken against employees who violate this directive</p>
<u>Human Resources</u>	<p>A. Provide guidance, as required, to City departments regarding appropriate disciplinary action to be taken against employees</p>

	who violate this directive
Attachments	
<u>N/A</u>	

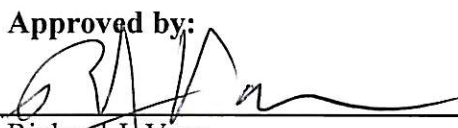
Information and/or clarification may be obtained by contacting the Information Technology Services Department (ITSD) at 207-8301.



 Hugh Miller
 Information Technology Services Department Director / CTO

09/14/2009

 Date

Approved by:


 Richard J. Varn
 Chief Information Officer (CIO)

09/16/2009

 Date

Approved by:


 Sheryl Sculley
 City Manager

9-29-09

 Date